REMARKS

Claims 1, 13, 14 and 26-30 have been amended.

The Examiner has rejected applicant's claims 1, 3, 6, 8-14, 16, 19 and 21-30 under 35 USC 103(a) as being unpatentable over the Anderson (U.S. Publication No. 2002/0052923) patent application publication in view of the Saliba, et al. (U.S. Publication No. 2001/0037315) patent application publication. The Examiner has rejected applicant's claims 4 and 17 under 35 USC 103(a) as being unpatentable over the Anderson publication in view of the Saliba, et al. publication in view of the McArdle (U.S. Pat. No. 6,442,686) patent. Applicant's claims 5 and 18 have been rejected under 35 USC 103(a) as being unpatentable over the Anderson publication in view of the Saliba, et al. publication and in view of the Baxter (U.S. Patent No. 6,385,306) patent. Applicant has amended applicant's independent claims 1, 13, 14 and 26-30 and with respect to these claims, as amended, and their respective dependent claims, the Examiner's rejections are respectfully traversed.

Applicant has amended applicant's independent claims 1, 13, 14 and 26-30 to better define applicant's invention. In particular, applicant's independent claims 1 has been amended to recite a communication system having a server for providing a Web E-Mail service to a client, wherein the server comprises management means for managing a key for decrypting an encrypted E-mail message addressed to a user's mail address, wherein the key for decrypting the encrypted E-mail message is not managed by the client, web encryption communication means for establishing a Web encryption communication with the client, and communicating with the client by the Web encryption communication established by the web encryption communication means, authentication means for executing authentication of a use allowance of

the key managed by the management means to the client when the client requests to decrypt the encrypted E-mail message while the server communicates with the client by the established Web encryption communication, decrypting means for decrypting the encrypted E-mail message using the key managed by the management means in the case where the use allowance of the key managed by the management means is authenticated by the authentication means, and transmission control means for controlling to transmit the E-mail message decrypted by the decrypting means to the client through the Web encryption communication established by the web encryption communication means. Applicant's independent claims 13, 14 and 26-30 have been similarly amended.

In addition, applicant's independent claim 13 has been further amended to recite the client comprising request means for requesting to decrypt the encrypted E-mail message while the Web encryption communication is established between the server and the client, authentication information sending means for sending the authentication information to the authentication means and receiving means for receiving the decrypted E-mail message transmitted by the transmission control means through the Web encryption communication established by the Web encryption communication means. Applicant's independent claims 26, 28 and 30 have been similarly amended.

The constructions recited in applicant's amended independent claims 1, 13, 14 and 26-30 are not taught or suggested by the cited art of record. In particular, the Examiner has argued that the Anderson publication teaches a communication system having a server for providing a Web E-mail service (Anderson: see for example, Para [0002] Line 3) to a client wherein said server comprises management means for managing a key for decrypting an encrypted E-mail (Anderson: Para [0002] Line 3, Para [0004] Line 10-21 and Para [0006] Line 1-15; the Email

server manages the key by authenticating the clients for access permission to Email). The Examiner has also argued that Anderson, in view of Saliba, et al., teaches authentication means for executing authentication of the use of allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail (Anderson: Para [0006] Line 10-15 and Para [0021] Line 11) while the server communicates with the client by the established Web encryption communication (Anderson: Para [0019] Line 6-10 & Saliba: Para[120] and decrypting the encrypted E-mail using the managed key (Anderson: see for example, Para [0006] Line 12).

Applicant has reviewed the passages of Anderson cited by the Examiner and believes that there is no teaching or suggestion in Anderson of managing a key for decrypting an encrypted E-mail message addressed to a user's mail address, wherein the key for decrypting the encrypted E-mail message is not managed by the client, of authenticating of a use allowance of the key managed by the management means to the client when the client requests to decrypt the encrypted E-mail message and of decrypting the encrypted E-mail message using the key managed by the management means if allowance of the key is authenticated. Specifically, Paragraphs [0002], [0004] and [0006] of the Anderson publication, cited by the Examiner, disclose an e-mail service (See, [0002]), problems associated with decentralized storage and management of electronic messages (See, [0004]), and a system (MDS) which uses centralized storage and management to track and manage requests from recipients to access the message by permitting access when appropriate and performing activities such as decrypting/encrypting the message (See, [0006]). These paragraphs of Anderson only generally disclose decrypting and encrypting of messages by the e-mail service system and permission of access to the message, and make no mention of managing of a key for decrypting an encrypted

E-mail message addressed to the user's mail address, wherein the key for decrypting the E-mail message is not managed by the client, of authenticating use allowance of this key when the client requests to decrypt the encrypted E-mail message and decrypting the encrypted E-mail message using this key if the key is authenticated.

Instead, the Anderson publication discloses that in response to a request from a message recipient to review a message, the message is transmitted from a server to the recipient after the server encrypts the message (if the original message was encrypted) with a public key of the recipient and the encrypted message is decrypted upon request by the recipient with a private key managed by the recipient. [Anderson, paragraph [0040], lines 16-24, paragraph [0044], lines 1-9]. Anderson also discloses that when the system receives a message to be distributed to one or more recipients, the system decrypts the message, if necessary, with the system's private key, stores the unencrypted message and creates a message indicator to be sent to each recipient with a reference to the stored message (See also, FIG. 5, Steps 510, 515, 520 and 533). Anderson further discloses that if the received message was encrypted, the system encrypts the message indicator using a public key for each recipient and sends the encrypted message indicator to each recipient (See, FIG. 5, Steps 540 and 545; Paragraphs [0039-0040]. The encrypted message indicator received by the recipient is then decrypted using the recipient's private key to allow the recipient to review the message (See, Paragraph [0044]).

Thus, in Anderson, when the recipient requests a message or a message indicator that are encrypted, decryption occurs with a private key which is managed by the client. The public keys managed by the system in Anderson are used only to decrypt the message for storage in the system's storage device and to encrypt the message indicator and/or message to the client. There is thus nothing is Anderson which can be equated to authentication of use allowance of

the key to the client when the client requests to decrypt the encrypted message and for decrypting an E-mail message if use allowance is authenticated. In Anderson, no such request is made for authentication of use allowance of a key managed by the server, and not by the recipient. Moreover, while Anderson permits access to messages when appropriate [Anderson, paragraph 0006], this is not a teaching or suggestion of authentication of use allowance of a key managed by the server, and not by the recipient.

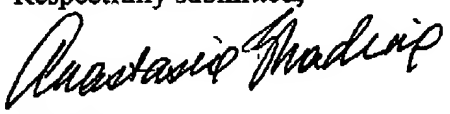
Applicant's amended independent claims 1, 13, 14 and 26-30, each of which recites managing a key for decrypting an encrypted E-mail message addressed to the user's mail address, wherein the key for decrypting the encrypted E-mail message is not managed by the client, executing authentication of a use allowance of the key managed by the management means to the client when the client requests to decrypt the encrypted E-mail message and decrypting the encrypted E-mail message using the key managed by the management means in the case where allowance of the key managed by the management means is authenticated, and their respective dependent claims, thus patentably distinguish over the cited Anderson publication. Moreover, the Saliba, et al. publication, which discloses decryption of SSL communications, and the McArdle and the Baxter patents fail to add anything to change this conclusion. Accordingly, applicant's amended independent claims 1, 13, 14 and 26-30, and their respective dependent claims patentably distinguish over the Anderson publication, the Saliba, et al. publication and the McArdle and the Baxter patents, taken alone or in combination.

In view of the above, applicant's independent claims 1, 13, 14 and 26-30, and their respective dependent claims, patentably distinguish over the cited art of record, and are

therefore submitted as patentable. Reconsideration of these claims is thus respectfully requested.

Dated: March 20, 2006

Respectfully submitted,



COWAN, LIEBOWITZ & LATMAN, P. C.
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200

Anastasia Zhadina
Reg. No. 48,544
Attorney of Record

25813/272/740460.1